Answer Key for Exam A

Section 1. Choose the correct answer:

1. What is data encryption standard (DES)?
   - [✓ (a)] block cipher
   - (b) stream cipher
   - (c) bit cipher
   - (d) none of the above
2. MAC address is of
   - (a) 24 bits
   - (b) 36 bits
   - (c) 42 bits
   - [✓ (d)] 48 bits
3. The special MAC broadcast address is
   - (a) AA-AA-AA-AA-AA-AA
   - (b) BB-BB-BB-BB-BB-BB
   - [✓ (c)] FF-FF-FF-FF-FF-FF
   - (d) 00-00-00-00-00-00
4. Which one of the following is the multiple access protocol for channel access control?
   - (a) CSMA/CD
   - (b) CSMA/CA
   - [✓ (c)] both (a) and (b)
   - (d) none of the above
5. VLANs may span multiple switches using
   - (a) home port
   - [✓ (b)] trunck port
   - (c) common port
   - (d) it is not possible at all
6. The maximum size of payload field in Ethernet frame is
   - (a) 1000 bytes
   - (b) 1200 bytes
   - (c) 1300 bytes
   - [✓ (d)] 1500 bytes
7. Header of a frame generally contains:
   - (a) synchronization bytes
   - (b) addresses
   - (c) frame identifier
   - [✓ (d)] all of the above
8. In asymmetric key cryptography, the private key is kept by
   - (a) sender
   - [✓ (b)] receiver
   - (c) sender and receiver
   - (d) all devices in the network

9. Cryptographic hash function takes an arbitrary block of data and returns
   - [✓ (a)] fixed size bit string
   - (b) variable size bit string
   - (c) both (a) and (b)
   - (d) none of the above
10. High speed Ethernet works on
    - (a) coaxial cable
    - (b) twisted pair cable
    - [✓ (c)] optical fiber
    - (d) none of the above
11. Listen before transmit is the logic of
    - (a) ALOHA
    - [✓ (b)] CSMA
    - (c) Slotted ALOHA
    - (d) TDMA
12. What is stat frame delimiter (SFD) in Ethernet frame?
    - (a) 10101010
    - [✓ (b)] 10101011
    - (c) 00000000
    - (d) 11111111
13. Pretty good privacy (PGP) is used in
    - (a) browser security
    - [✓ (b)] email security
    - (c) FTP security
    - (d) all of the above

Section 2. Match the operation with the corresponding purpose.

(c)	Get fixed size message digest	(a) $K_s(m), K_B^+(K_s)$
(b)	Public Key Encryption	(b) $K_B^+(m)$
(h)	Digital signature Verification	(c) $H(m)$
(g)	Symmetric Key Decryption	(d) $K_B^-(H(m))$
(f)	Symmetric Key Encryption	(e) $K_B^-(K_B^+(m))$
(a)	Sending a confidential email (m) to Bob	(f) $K_s(m)$
(e)	Public Key Decryption	(g) $K_s(K_s(m))$
(d)	Digital signature	(h) $K_B^+(K_B^-(H(m)))$

Section 3. Answer the following questions.

1. The Services Provided by the Link Layer are:

   Framing

   Link Access

   Reliable delivery

   Error detection and correction

2. Where Is the Link Layer Implemented?

link layer implemented in adaptor (network interface card NIC) or on a chip

3. For CRC, assume that D=0101101010 and G=10011 , then R=

1111

4. Consider RSA with $p = 11$ and $q = 13$.

a. What are n and z?

$n = pq = 143$

$z = (p - 1)(q - 1) = 120$

b. Let $e = 7$. Why is this an acceptable choice for e?

They are relatively prime. Because the prime factors of $z = 120$ are $2, 3, 5$ do not include 7.

c. Find d such that $de = 1(mod z)$ and $d < 110$.

$d = 103$

d. Encrypt the message $m = 4$ using the $key(n, e)$. Let c denote the corresponding ciphertext.

$c = m^e mod n = 4^7 mod 143 = 82$

e. Why RSA is secure?

Because, it is so difficult to factorize a large integer n into its prime factors p, q.

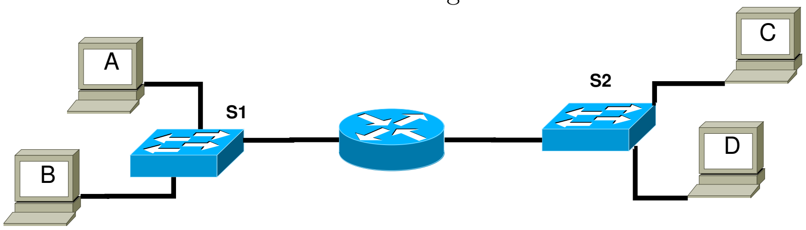
5. Mark the error in the following Two-dimensional even parity.

1	0	1	1	0	0	1	||	0
1	0	1	0	0	0	1	||	0
0	1	1	0	1	1	0	||	1
−−	−−	−−	−−	−−	−−	−−		
1	1	0	0	0	1	1	||	0

When does this technique fail to detect error?

When an even number of errors occurs in the same row or the same column

6. Consider the network shown in the figure below.



Suppose A would like to send an IP datagram to D, and assume that A's ARP cache does not contain D's MAC address.

Will A perform an ARP query to find D's MAC address? Why?

No, because they are not on the same LAN.

A can find out that they are not on the same subnet by checking D's IP address.

In the Ethernet frame (containing the IP datagram destined to D) that is delivered to router, what are the source and destination IP and MAC addresses?

Ethernet frame from A to D: Source IP = A's IP address Destination IP = D's IP address

Source MAC = A's MAC address

Destination MAC = The MAC address of router's interface connecting to Subnet containing A

Suppose Host A would like to send an IP datagram to Host B, and neither A's ARP cache contains B's MAC address nor does B's ARP cache contain A's MAC address. Further suppose that the switch forwarding table contains entries for Host B and the router only. Thus, A will broadcast an ARP request message. What actions will the switch perform once it receives the ARP request message?

Switch S1 will broadcast the Ethernet frame via both its interfaces

as the received ARP frame's destination address is a broadcast address.

And it learns that A resides on Subnet 1 which is connected to S1 at the interface connecting to Subnet 1

And, S1 will update its forwarding table to include an entry for Host A

Will router also receive this ARP request message? If so, will forward the message to the other Subnet?

Yes, router R1 also receives this ARP request message, but R1 won't forward the message to Subnet 3.

Once Host B receives this ARP request message, it will send back to Host A an ARP response message. But will it send an ARP query message to ask for A's MAC address? Why?

B won't send ARP query message asking for A's MAC address,
as this address can be obtained from A's query message.

What will the switch do once it receives an ARP response message from Host B?

Once switch S1 receives B's response message,
it will add an entry for host B in its forwarding table, and then drop the received frame
as destination host A is on the same interface as host B (i.e., A and B are on the same LAN segment).

7. Suppose four active nodes—nodes A, B, C and D—are competing for access to a channel using slotted ALOHA. Assume each node has an infinite number of packets to send. Each node attempts to transmit in each slot with probability p. The first slot is numbered slot 1, the second slot is numbered slot 2, and so on.

a. What is the probability that node A succeeds for the first time in slot 5?

$(1-p(A))^4 p(A)$
where, $p(A)$ = probability that A succeeds in a slot
$p(A)$ = p(A transmits and B does not and C does not and D does not)
= p(A transmits) p(B does not transmit) p(C does not transmit) p(D does not transmit)
$= p(1-p)(1-p)(1-p) = p(1-p)^3$
Hence, p(A succeeds for first time in slot 5)
$= (1-p(A))^4 p(A) = (1-p(1-p)^3)^4 p(1-p)^3$

b. What is the probability that some node (either A, B, C or D) succeeds in slot 4?

p(A succeeds in slot 4) $= p(1-p)^3$
p(B succeeds in slot 4) $= p(1-p)^3$
p(C succeeds in slot 4) $= p(1-p)^3$
p(D succeeds in slot 4) $= p(1-p)^3$
p(either A or B or C or D succeeds in slot 4) $= 4p(1-p)^3$ (because these events are mutually exclusive)

c. What is the efficiency of this four-node system?

efficiency = p(success in a slot) $=4p(1-p)^3$